Supreme Court, U.S.
FILED

(1)

No. 02 818 NOV 26 2002

OFFICE OF THE CLERK

In The

Supreme Court of the United States

DAVID WESLEY HAWKINS,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Petition For Writ Of Certiorari To The Supreme Court Of California

PETITION FOR WRIT OF CERTIORARI

ANDREW PARNES
Counsel of Record
160 Second Street East
P.O. Box 5988
Ketchum, Idaho 83340
Phone (208) 726-1010

Attorney for Petitioner

November 26, 2002

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

MHPP

QUESTIONS PRESENTED

I. Whether a statute criminalizing the copying of computer data fails to give adequate notice to citizens and law enforcement and is therefore unconstitutionally vague where the language of the statute prohibits the prosecution of acts which may "incidentally violate" the law.

II. Whether a defendant's right to a fair trial is violated when the trial court admits evidence of a prior act involving the defendant's alleged possession of computer code, where there was no proof that the code was protected or that the possession of the code was illegal.

III. Whether a jury must be instructed on the requirement of unanimously agreeing that the defendant violated the statute when there are multiple and distinct acts on which the jury could have relied for conviction.

TABLE OF CONTENTS

	Page
QUESTIONS PRESENTED	i
OPINIONS BELOW	1
STATEMENT OF JURISDICTION	1
CONSTITUTIONAL AND STATUTORY PROVISIONS	1
STATEMENT	3
REASONS FOR GRANTING THE PETITION	8
1. THE STATUTE PROHIBITING THE PROSECUTION OF ACTS WHICH MAY "INCIDENTALLY VIOLATE" THE OTHER PROVISIONS OF THE LAW IS UNCONSTITUTIONALLY VAGUE	8
2. ADMISSION OF A PRIOR ACT AT TRIAL WHERE THERE IS NO PROOF THAT THE ACT WAS ILLEGAL VIOLATES A DEFENDANT'S RIGHT TO A FUNDAMENTALLY FAIR TRIAL	13
3. THE FAILURE TO INSTRUCT THAT JURORS MUST UNANIMOUSLY AGREE ON WHICH OF MORE THAN ONE ACT CONSTITUTED A VIOLATION OF THE STATUTE DENIED PETITIONER HIS CONSTITUTIONAL RIGHTS	17
CONCLUSION	21

TABLE OF AUTHORITIES

Page

FEDERAL CASES

Chicago v. Morales, 527 U.S. 41, 119 S. Ct. 1849, 144 L. Ed. 2d 67 (1999) 9

Estelle v. McGuire, 502 U.S. 62, 112 S. Ct. 475, 116 L. Ed. 2d 385 (1991) 14

Huddleston v. United States, 485 U.S. 681, 108 S. Ct. 1496, 99 L. Ed. 2d 771 (1988) 14

Kolender v. Lawson, 461 U.S. 352, 103 S. Ct. 1855, 75 L. Ed. 2d 903 (1983) 9, 11, 12

McKoy v. North Carolina, 494 U.S. 433, 110 S. Ct. 1227, 108 L. Ed. 2d 369 (1990) 18

Richardson v. United States, 526 U.S. 813, 119 S. Ct. 1707, 143 L. Ed. 2d 985 (1999) 19

Schad v. Arizona, 501 U.S. 624, 111 S. Ct. 2491, 115 L. Ed. 2d 555 (1991) 17, 18, 19

Smith v. Goguen, 415 U.S. 566, 94 S. Ct. 1242, 39 L. Ed. 2d 605 (1974) 9

Walters v. Maass, 45 F.3d 1355 (9th Cir. 1995) 14

In re Winship, 397 U.S. 358, 90 S. Ct. 1068, 25 L. Ed. 2d 368 (1970) 17

STATE CASES

People v. Davis, 8 Cal. App. 4th 28 (1992) 17

People v. Hawkins, 98 Cal. App. 4th 1428 (2002) 1

People v. Thompson, 36 Cal. App. 4th 843 (1995) 17

Williams v. Garcetti, 5 Cal. 4th 561 (1993) 12

TABLE OF AUTHORITIES – Continued

Page

FEDERAL STATUTES

28 U.S.C. § 1257(3) 1

STATE STATUTES

California Penal Code § 272 12
California Penal Code § 499c 3
California Penal Code § 502 12
California Penal Code § 502(c)(2) 1
California Penal Code § 502(h) 10
California Penal Code § 502(i) 10
California Penal Code § 12022.6 3

OPINIONS BELOW

The opinion of the Court of Appeal of the State of California is published at *People v. Hawkins*, 98 Cal. App. 4th 1428 (2002). A copy of the opinion is attached hereto in the Appendix at App. 1. On July 2, 2002, the Court of Appeal denied rehearing and modified its opinion without changing the judgment. A copy of the modified opinion is attached hereto in the Appendix at App. 40. The California Supreme Court denied a timely petition for review in an unpublished order dated August 28, 2002. A copy of the denial is attached hereto in the Appendix at App. 43.

STATEMENT OF JURISDICTION

This Court has jurisdiction to consider this case pursuant to 28 U.S.C. § 1257(3).

CONSTITUTIONAL AND STATUTORY PROVISIONS

United States Constitution, Amendment 14:

"[N]or shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

California Penal Code section 502(c)(2):

> (c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

* * *

(c)(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

* * *

(d)(1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

* * *

(h)(1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or provided that the value of supplies or computer

services, as defined in paragraph (4) of subdivision (b), which are used does not exceed an accumulated total of one hundred dollars ($100).

* * *

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

STATEMENT

Petitioner David Wesley Hawkins was charged in the California state court with one count of misappropriation of a trade secret in violation of California Penal Code § 499c and one count of knowingly accessing and without permission taking, copying or making use of data from a computer system in violation of California Penal Code § 502(c)(2). Both counts contained allegations that the property taken exceeded a value of $2.5 million under California Penal Code § 12022.6.

At jury trial on these charges, the jury acquitted Mr. Hawkins of the trade secret charge, but returned a guilty verdict on the copying computer data count. The jury found not true the excessive taking allegation. After denying a motion for new trial, the court placed Mr. Hawkins on three years probation on condition that he serve six months in the county jail.

Timely notice of appeal was filed and the California Court of Appeal affirmed the conviction. Mr. Hawkins' timely Petition for Review was denied by the California Supreme Court.

In 1995, Mr. Hawkins was employed at a small start-up company, NTI, Inc., which developed and manufactured a firewall device for Internet users. (RT 113.) This device, named PIX, sought to protect Internet users from external access by other Internet users. Mr. Hawkins was hired to provide technical engineering assistance to NTI customers. (RT 113.) As part of his duties in providing technical assistance for NTI, Mr. Hawkins had access to the source code of the PIX program. (RT 136-137.) Other employees also had access to this code. (RT 137.)

After Mr. Hawkins began his employment at NTI, the company was purchased by Cisco in late October 1995. Mr. Hawkins, along with other NTI employees, continued his work in technical support at Cisco until he informed the company that he would leave on August 16, 1996. (RT 142, 144.)

The field for firewall devices was highly competitive and early entrance into the market was a key factor in PIX's value to Cisco. At the time of the NTI purchase, the main firewall provider was a company called Checkpoint. (RT 184-185.) Within the next year, there were numerous companies competing in the firewall market. (RT 135-136, 162-163, 186, 308.)

While employed at Cisco in early 1996, Mr. Hawkins met with two other individuals, Debbie Appler and Larry Coryell, to discuss the formation of a company to compete with and advance upon the PIX product, now owned by Cisco. (RT 283-284, 912.) Being intimately familiar with the functioning of the PIX product, Mr. Hawkins hoped to develop a better product. (RT 300-301, 912-913.) Ms. Appler was primarily a marketing person and Mr. Coryell was a programmer. (RT 285, 919-920.) Mr. Hawkins

provided to Mr. Coryell block diagrams of the functions sought to be developed for the new product and Mr. Coryell developed software programs for the product beginning in early April 1996. (RT 920, 927.) Mr. Coryell independently obtained employment with a different branch of Cisco during this period and worked on the venture with Mr. Hawkins in the evenings. (RT 922.) By the fall of 1996, Mr. Coryell had stopped working on the venture, partly for health reasons and partly because he did not believe that the product would ever be marketed. (RT 948, 992, 1011.)

Mr. Hawkins continued with the project and formed a company called Meridian Network Systems in 1997. With others, he began to market a product called Aegis which would be a competitor to PIX. In May 1997, John Mayes attended a computer show in Las Vegas and saw Mr. Hawkins at the Meridian booth. (RT 145.) Mayes became concerned that the Meridian product was similar to PIX and contacted lawyers at Cisco. Upon his return to the Bay Area, Mr. Mayes purchased an Aegis and had people compare the two products. Based upon this comparison, Cisco believed that its proprietary information may have been used to develop Aegis. (RT 157-161.)

On August 8, 1997, a search warrant was issued and served on Mr. Hawkins' home office. Investigator John Smith and a computer expert, Gordon Galligher, who was retained by Cisco, searched the premises and downloaded information from Mr. Hawkins' computers. Two directories, labeled DWH/SRC/NTI/2.7.6 and DWH/SRC/NTI/2.6.102, were found on one of the computers. (RT 597.) These files contained source code of the PIX programs.

Mr. Galligher testified that during the execution of the warrant Mr. Hawkins was cooperative and assisted them

in gaining access to the machinery. After the PIX code was found, Mr. Hawkins continued to cooperate with the investigation and told the investigators that he always made a backup tape of his home directory when leaving a company to make sure that he has standard start-up files, and if he had copied Cisco source code, it was completely by accident. Mr. Hawkins denied making any use of the source code in creating his Aegis product. (RT 602.)

Mr. Galligher later compared the two source codes for PIX and Aegis and testified that he could form no conclusion that the two were the same, in part because they were written in different programming languages. (RT 616.) Mr. Galligher believed that the two programs might have a common ancestry. (RT 583, 697.) However, after this initial conclusion, he reviewed the programs as well as the history of the development of Aegis at the request of Mr. Hawkins' counsel and determined that he could not conclude that Aegis had used PIX as a starting point. (RT 743.) He further learned that Mr. Coryell, not Mr. Hawkins, was the principal developer of the Aegis program and that the programing was begun before Mr. Hawkins left Cisco. (RT 648-651; 761-762.)

Mr. Coryell acknowledged that he wrote the main part of the Aegis source code and began the program in April 1996. (RT 921; 977.) Mr. Hawkins never mentioned the PIX source code to him, and Mr. Coryell developed the Aegis code without looking at the PIX code. (RT 986, 996.) While Mr. Coryell was working on the code, all Mr. Hawkins did was write a low-level driver code for the program. (RT 995.) Mr. Coryell testified that after Mr. Hawkins left Cisco, Mr. Hawkins appeared to spend more time on developing the product. Mr. Coryell provided little

assistance during the fall of 1996, because he was undergoing chemotherapy. (RT 999-1000.)

Mr. Galligher testified that the access dates on the PIX source code files on Mr. Hawkins' computer were in December 1996 and May 1997. Regarding the December 1996 access, he concluded that since all of the files showed an access on that date, the implication was that the machine was simply backed up on that date and this "absolutely supported the potential that it was an accident." (RT 645.) Thus, he could not conclude that someone accessed the files intentionally on that date. Nor could he determine who accessed the files from the information provided, since Mr. Hawkins' computers were accessible by Internet and thus users other than Mr. Hawkins had direct access to the computer. (RT 807-808.) The first step taken at the execution of the warrant was to disconnect the computer from the Internet to secure it and to prohibit outside users from contacting the computer. (RT 584, 799.) Because the computer was not protected by a firewall or a password, anyone connecting to the computer through the Internet would have direct access to the machine and an ability to load or modify files onto the machine. (RT 808.)

Mr. Galligher further opined that the May 15, 1997, access data were different from the December access data because only one file related to source code appeared to be accessed on 5-17-97, even though numerous other non-source code files appeared to have been accessed that day. (RT 645; 837.) None of these files was connected to the creation of a source code similar to PIX. Only one PIX file showed an access date after December 1996. (RT 645.) Mr. Galligher acknowledged that during the execution of the warrant information regarding access to directories and files was lost. (RT 837.)

Andrew Foss, an employee of NTI, testified over objection that, after the purchase by Cisco, in working with Mr. Hawkins on a particular computer program function, Mr. Hawkins showed him an example of that function in the Sun Operating System source code. (RT 442.) Mr. Foss was able to identify the Sun code because he had access to it in a prior job. (RT 440.) But Mr. Foss did not know whether part of the code he saw was in the public domain at that time. He acknowledged that much of the Sun code was based on free Berkeley Software Distribution (B.S.D.) Unix which is available for distribution on the Internet. Mr. Foss believed that certain Sun O.S. files are identical to free B.S.D. files. (RT 454.) While Mr. Foss did not know whether the files he observed had entered the public domain, he did acknowledge that headers identifying the writer and owner of the code are often retained at the top of the code. (RT 453.)

Mr. Foss recalled that Mr. Hawkins mentioned that the code was in his home directory and that he moved his home directory to his machine at Cisco. (RT 443; 456.) Mr. Foss stated that he had "no reason to believe that [having the file] was inadvertent or on purpose." (RT 443.)

REASONS FOR GRANTING THE PETITION

1. THE STATUTE PROHIBITING THE PROSECUTION OF ACTS WHICH MAY "INCIDENTALLY VIOLATE" THE OTHER PROVISIONS OF THE LAW IS UNCONSTITUTIONALLY VAGUE

Mr. Hawkins stands convicted, following a jury trial, of violating a complex state criminal statute related to the copying of computer data. Given the pervasive use of

computers in our modern society, it is essential that laws which criminalize the use of computers be sufficiently clear to inform computer users of those acts which are illegal. This is especially important in the area of laws which regulate the copying of computer data because one of the tremendous benefits of computer technology is the almost instantaneous transfer of information from one computer to another.

The California statute is written with a broad brush and makes illegal "all copying" of computer data "without permission." Probably realizing the dangerous sweep of this language, the California legislature attempted to place some limits on this broad definition. However, the legislature's attempt to narrow the statute, by prohibiting the prosecution of persons who "incidentally violate" the provisions of the statute, created statutory language which is itself unconstitutionally vague.

The constitutional interest implicated in questions of statutory vagueness is that no person be deprived of "life, liberty, or property without due process of law," as assured by the Fourteenth Amendment. "As generally stated, the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357, 103 S. Ct. 1855, 75 L. Ed. 2d 903 (1983). Thus, a criminal statute must "establish minimal guidelines to govern law enforcement." *Smith v. Goguen*, 415 U.S. 566, 574, 94 S. Ct. 1242, 39 L. Ed. 2d 605 (1974); *Chicago v. Morales*, 527 U.S. 41, 119 S. Ct. 1849, 144 L. Ed. 2d 67 (1999).

Penal Code § 502(c)(2) prohibits a person from knowingly accessing and without permission taking, copying or making use of any data from a computer system. However, the statute attempts to exempt from prosecution a broad range of conduct. First, the preceding statute does not apply to any person acting within the scope of his or her lawful employment. California Penal Code § 502(h). Second, the statue does not apply to any employee who acts *outside* the scope of his or her lawful employment "so long as the employee's activities do not cause injury . . . or so long as the value of the supplies or computer services . . . does not exceed an accumulated total of one hundred dollars." California Penal Code § 502(h). Finally, the statute exempts from *prosecution* any activity which "incidentally violates" subdivision (c)(2). Cal. Penal Code § 502(i).

The state appellate court described the statute as creating "a relatively new computer crime" which "describes a number of computer crimes in somewhat overlapping language and [creating] several exemptions from prosecution." App. 1, 11, 16. There can be no question that this statute is "complex" (App. 16) and that it contains numerous exemptions, which are not only potential affirmative defenses but act to bar prosecution for certain conduct.

The critical question is whether this statute provides proper notice to both the citizen and the police to guide their respective conduct. The statute is so broad that law abiding employees who work daily with computers are unable to determine which of their acts is prohibited or exempted by this statute. Millions of employees access computers, computer networks and the Internet every day. Data is transferred from computer to computer, or from

computer to disk, every second of the work day. Material is taken, copied and made use of in most of these transactions. The statute provides insufficient guidance to permit the computer users to know if their acts are legal or illegal.

There exists no basis for a reasonable person to discern when his or her access to a computer or system only "incidentally violates" the statute and is thus *exempt* from prosecution. In addition, there exists no rational basis on which the prosecutor can make his or her decision to prosecute under the statute. Though the legislature obviously intended to exclude certain routine copying from prosecution, the language used by the legislature fails to protect these interests in a manner that is not void-for-vagueness.

For example, the statute can easily be violated by an unwitting computer user – by pushing the wrong button which causes information to be displayed, copied, or downloaded. However, the statute makes no provision for such accidental or unintentional use once the person knowingly accesses the computer.

Additionally, under the statute, prosecution could be brought for copying innocuous data from a computer, such as recipes, e-mails, photographs and other trivial information, all of which are covered under the broad definition of subdivision (c)(2).

In *Kolender*, this Court voided a California statute requiring individuals to provide "credible and reliable" identification to a police officer. In rejecting this statutory language as vague, this Court held that neither the statute nor the construction of the state courts contained "a standard for determining what a suspect has to do in

order to satisfy the requirement to provide a 'credible and reliable' identification." *Kolender*, 461 U.S. at 358. No state court has established a construction of the "incidentally violates" language in the computer copying statute. Nor does the statute itself attempt to define this language. Instead, the definition of the term is left up to the individual police officer or prosecutor who decides to either arrest or prosecute a person under this code section. What is "incidental" to one person may not be "incidental" to another. Because of the wide range of possible interpretations of this language, neither the citizens nor law enforcement agents are provided even minimal standards for determining when a violation of the statute occurs.

In *Williams v. Garcetti*, 5 Cal. 4th 561 (1993), the California Supreme Court rejected a vagueness challenge to a 1988 amendment to California Penal Code § 272 which required parents and guardians of children under 18 "to exercise reasonable care, supervision, protection, and control over their minor child." The court found the language of the statute met constitutional due process requirements "because it incorporates the definitions and the limits of parental duties that have long been a part of California dependency law and tort law." *Id.* at 570. The court went on to cite a long line of statutes and case law defining the terms "supervision" and "control." *Id.* at 570-572.

In contrast here, no such extensive analysis exists for the "incidentally violates" language in section 502. The Court of Appeal did not cite to any case in either California or elsewhere which has interpreted the word "incidentally" in any manner which gives clear guidance to either the prosecutor "who shall not prosecute" or the defendant whose actions may be subject to criminal liability.

The dangers of this statute are vividly portrayed here where Mr. Hawkins was *acquitted* of the specific and definite crime of theft of a trade secret *and* the jury could place no value on the data they found was improperly copied. Because the statute provides no guidance as to whether Mr. Hawkins' actions may have only "incidentally" violated the statute, Mr. Hawkins should never have been prosecuted. Yet, he now stands convicted and faces a significant jail term for conduct which may have been barred from prosecution under the statute.

2. ADMISSION OF A PRIOR ACT AT TRIAL WHERE THERE IS NO PROOF THAT THE ACT WAS ILLEGAL VIOLATES A DEFENDANT'S RIGHT TO A FUNDAMENTALLY FAIR TRIAL

During trial, the prosecution introduced, over objection, the testimony of Andrew Foss, who claimed to have once seen source code from another computer company on Mr. Hawkins' computer. This evidence was used to prove that Mr. Hawkins had taken code from another company before and thus did not inadvertently possess the code he was charged with taking in this case. At the hearing on the admission of this evidence, the trial court ruled that

> [the prosecutor] has to prove that in fact, it was a source code which was not readily available, was protected, was not a source code that was to be taken from the premises by an employee, et cetera, et cetera. If he doesn't prove that, then you [defense counsel] are right; there is no value whatsoever. It's not a prior act. It can't be argued as a prior act, et cetera. . . . [U]nless [the prosecutor] can prove it up it has no value, and I assume from your offer of proof that you can prove

> it up. . . . That's the point. If you [the prosecutor] can't prove it up, it's absolutely irrelevant.

(RT 44-46.)

While Foss testified that he believed what he had seen was "source code," he was not certain what parts of the code he had observed. More importantly, he could not state that the items he had seen were held confidentially by the computer company or whether they had been released into the public domain at the time he saw them. Thus, the prosecution failed to meet its burden, and the admission of this irrelevant evidence denied Mr. Hawkins a fundamentally fair trial as guaranteed by his right to due process under the Fourteenth Amendment to the United States Constitution. *Estelle v. McGuire*, 502 U.S. 62, 70, 112 S. Ct. 475, 116 L. Ed. 2d 385 (1991); *Walters v. Maass*, 45 F.3d 1355, 1357 (9th Cir. 1995).

The state appellate court erroneously upheld the admission of the evidence on the basis that Foss's speculative testimony was sufficient to meet the requirements outlined by the trial court. If this approach to the issue of prior act evidence is permitted to stand, the fundamental basis for the admission of prior act evidence will be eviscerated.[1] The prosecution will be permitted to introduce

---

[1] In the context of interpreting the Federal Rules of Evidence, this Court has stated that the Government "may [not] parade past the jury a litany of potentially prejudicial similar acts that have been established or connected to the defendant only by unsubstantiated innuendo. . . . similar act evidence is relevant only if the jury can reasonably conclude that the act occurred and that the defendant was the actor." *Huddleston v. United States*, 485 U.S. 681, 689, 108 S. Ct. 1496, 99 L. Ed. 2d 771 (1988). In *Huddleston*, the evidence was relevant only if the jury could conclude that the televisions at issue were actually

(Continued on following page)

evidence of prior bad acts or crimes which is wholly unsupported by facts. For example, in an auto theft case it would be sufficient for a witness to testify that he saw the defendant in another's automobile at a prior time as evidence that the defendant intended to steal a car in a later case. The prosecution would not even have to bring the owner of the automobile forward to state that the defendant did not have permission to drive the car or that the car was stolen at the time the defendant was driving that car. In the instant case, no one testified that the code seen by Foss, if it indeed was even source code, was held by Mr. Hawkins unlawfully or without permission.

The state appellate court went on to hold that *even if* Foss was uncertain that he had seen source code, his testimony was relevant as a prior "caution" about the possession of protected code in general. App. 21. Cautioning a person about the possible illegality of an act does not meet the test of relevance and the admission of the Foss testimony under this theory violates the Due Process Clause of the Fourteenth Amendment. A prior "caution," if indeed the recipient is even aware of the caution, does not have a tendency to prove that the recipient later had the intent to violate the law. Haven't we all been warned by our parents not to speed or break the law?

Moreover, this theory of prior caution was not the subject of the prosecution's offer of proof for the evidence admitted against Mr. Hawkins. As the trial court noted,

---

stolen. Under the facts of that case, this Court found that there was sufficient evidence presented to support that conclusion. In contrast, here there is no sufficient evidence to support the conclusion that Mr. Hawkins possessed *protected* code.

unless the prosecution could prove that Mr. Hawkins unlawfully possessed Sun source code that "was not readily available, was protected, . . . , there is no value whatsoever. It's not a prior act." (RT 44.) The trial court would never have permitted Foss to testify about a general warning.

That the evidence was prejudicial cannot be contested. Foss' testimony was the lynchpin of the prosecution's case on the copying charge. The prosecutor stressed the importance of this evidence in closing argument. (RT 1054; 1061 ["Exactly the same thing he'd said to Andrew Foss about the Sun O.S. operating system."]; 1069 ["And then, finally, relative to this, the Sun O.S. incident, I think it's fair to infer that Mr. Hawkins took with him when he left more source code that he thought might be interesting in the future; because he did it twice."]; 1071 ["His claim that it was inadvertent is belied by the fact that the last thing he'd do is be casual about that data. That's what I meant with by number one by the frequent accesses that occurred after the data was taken and by the incident with the Sun O.S. system, that operating system source code, that occurred only a few months before."]) The prosecutor exploited the Foss testimony to undermine Mr. Hawkins' defense that his possession of the PIX source code was inadvertent. Because the state's evidence against Mr. Hawkins was circumstantial and not compelling, the state's reliance on speculative prior act evidence to "prove" to the jury that Mr. Hawkins had the propensity to intentionally take source code was not harmless.

3. THE FAILURE TO INSTRUCT THAT JURORS MUST UNANIMOUSLY AGREE ON WHICH OF MORE THAN ONE ACT CONSTITUTED A VIOLATION OF THE STATUTE DENIED PETITIONER HIS CONSTITUTIONAL RIGHTS

In this case, the prosecution contended that Mr. Hawkins copied and made use of two separate source code programs. In addition, in arguments to the jury the prosecution relied both upon (1) a taking and (2) a distinct use of the codes. Neither the prosecutor's argument nor any jury instructions informed the jury that they had to unanimously agree on whether the code was taken or used or which of the two separate codes was taken and copied.

In California, all twelve jurors must agree to return a guilty conviction. "It is fundamental that a criminal conviction requires a unanimous jury verdict." *People v. Thompson,* 36 Cal. App. 4th 843, 851 (1995); *In re Winship,* 397 U.S. 358, 90 S. Ct. 1068, 25 L. Ed. 2d 368 (1970). "What is required is that the jurors unanimously agree defendant is criminally responsible for 'one discrete criminal event.'" *Thompson, supra*, 36 Cal. App. 4th at 851, quoting *People v. Davis*, 8 Cal. App. 4th 28, 41 (1992).

In *Schad v. Arizona*, 501 U.S. 624, 111 S. Ct. 2491, 115 L. Ed. 2d 555 (1991), this Court held that the failure to require a unanimity instruction on alternate theories of first degree murder did not violate the Due Process Clause. "Plainly there is no general requirement that the jury reach agreement on the preliminary factual issues which underlie the verdict." *Id.* at 632. "That is not to say, however, that the Due Process Clause places no limits on a State's capacity to define different courses of conduct, or states of mind, as merely alternative means of committing

a single offense, thereby permitting a defendant's conviction without jury agreement as to which course or state actually occurred." *Ibid.*

The majority in *Schad* cited to a concurring opinion of Justice Blackmun in *McKoy v. North Carolina*, 494 U.S. 433, 449, 110 S. Ct. 1227, 108 L. Ed. 2d 369 (1990) (Blackmun, J, concurring.) Justice Blackmun wrote in *McKoy*:

> There is one significant exception to this principle. . . . In federal criminal prosecutions, where a unanimous verdict is required, the Courts of Appeals are in general agreement that "[u]nanimity . . . means more than a conclusory agreement that the defendant has violated the statute in question; there is a requirement of substantial agreement as to the principal factual elements underlying a specified offense." *United States v. Ferris*, 719 F2d 1405, 1407 (CA9 1983). *Accord, United States v. Duncan*, 850 F2d 1104, 1110-1115 (CA6 1988); *United States v. Beros*, 833 F2d 455, 461 (CA3 1987); *United States v. Schiff*, 801 F2d 108, 114 (1986), cert denied, 480 US 945, 94 L Ed 2d 789, 107 S Ct 1603 (1987); *United States v. Gipson*, 553 F2d 453, 456-459 (CA5 1977). But see *United States v. Bouquett*, 820 F2d 165, 169 (CA6 1987) (questioned in *Duncan*, 850 F2d, at 1112-1113). This rule does not require that each bit of evidence be unanimously credited or entirely discarded, but it does require unanimous agreement as to the nature of the defendant's violation, not simply the fact that a violation has occurred.

Id. at 449, n. 5.

In his concurring opinion in *Schad*, Justice Scalia noted that "[w]e would not permit, for example, an indictment charging that the defendant assaulted X on Tuesday or Y on Wednesday. . . . " *Schad v. Arizona*, 501 U.S. at 651.[2] Yet, this is precisely the error in the failure to provide a unanimity instruction here.

In this case, there were at least two distinct codes and two distinct acts which could have formed the basis of the single charge. Indeed, at the preliminary hearing, the prosecution's proof was separate and distinct from the proof at trial. At preliminary hearing, the prosecution relied upon Mr. Hawkins' alleged possession of a Cisco password and a "netsnoop" program for proof of Count Two. (CT 9, 256.) The prosecutor contended that Mr. Hawkins did not obtain the source code by violating section 502(c), but "in a more conventional way by downloading to a floppy disk or disk drive and simple asportation." (CT 256.)

Before trial, the prosecution was permitted to amend the information, now asserting that Mr. Hawkins copied and used the PIX code. (CT 783.) While this amendment may have provided notice to Mr. Hawkins of the general change in the prosecution's case, it cannot replace the duty of the prosecution to make an election at a point before the closing arguments or to inform the jury of the unanimity requirement.

---

[2] This language was cited with approval in *Richardson v. United States*, 526 U.S. 813, 820, 119 S. Ct. 1707, 143 L. Ed. 2d 985 (1999), a case requiring a specific unanimity instruction in a continuing criminal enterprise case where the government must prove each of the underlying violations.

During pre-trial motions, the prosecutor relied on both Mr. Hawkins' copying and use of the code as a basis for Count Two. (CT 861.) The prosecutor indicated that he could present two separate criminal acts to support Count Two as long as the court gave a unanimity instruction. (CT 865.) Ultimately, however, the court failed to give this instruction that even the prosecutor had acknowledged was proper in this circumstance.

Moreover, the prosecutor did not consistently select a specific act for Count Two before the closing argument, after the conclusion of the presentation of evidence. Instead, the prosecution argued that there was no statutory requirement that the accessing occur simultaneously with the taking, copying or using. "[I]t would be a practical impossibility for the actor to *make use* of the data during the time period of the access." (CT 864 [emphasis in original].) The prosecutor also argued that acts outside the time period charged could be considered. "I don't believe the time frame of the complaint is of the essence in a criminal pleading anyway."[3] (RT Augmentation, 7.) Finally, because the jury was instructed that the prosecution need not show that the crime was committed on a particular date, the jury should have been instructed that it had to unanimously agree on the specific acts which occurred to violate the law. *See* CALJIC 4.71.5 (requiring the jury to unanimously agree upon the commission of the same specific act or acts constituting the crime where the information charges an act or series of acts within a

[3] Mr. Hawkins' motion to dismiss for alleging acts outside the charging period was denied.

specified period and the prosecution has not elected to rely upon any specific date or dates).

Here, the prosecution failed to maintain a consistent theory of liability throughout the prosecution of Mr. Hawkins, argued two different theories as to how Mr. Hawkins violated the law (i.e., taking and copying vs. using), and argued that acts outside the time frame of the information could be relied upon by the jury. Accordingly, a unanimity instruction was constitutionally required in this case. The trial court's failure to so instruct the jury violated Mr. Hawkins' due process right to a fair trial in violation of the Fourteenth Amendment.

CONCLUSION

For the foregoing reasons, Petitioner respectfully requests that this Court grant certiorari and reverse his conviction.

Respectfully submitted,

ANDREW PARNES
Counsel of Record
160 Second Street East, Suite 216
Ketchum, ID 83340
(208) 726-1010

COPY

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL
OF THE STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

THE PEOPLE, Plaintiff and Respondent, v. DAVID WESLEY HAWKINS, Defendant and Appellant.	H021902 (Santa Clara County Super. Ct. No. 210319) (Filed June 5, 2002)

After hearing testimony for six days, a jury acquitted David Hawkins of a charge of misappropriating a trade secret (count 1; Pen. Code, § 499c)[1] and convicted him of a relatively new computer crime, the felony of knowingly accessing and taking data from a computer system (count 2; § 502, subd. (c)(2)). The jury found not true that the property taken, source code, was valued at more than $2.5 million. (§ 12022.6, subd. (a)(4).)

The trial court denied defendant's motions for a new trial and to reduce the offense to a misdemeanor. The court suspended imposition of sentence and placed defendant on formal probation for three years, on condition, among others, that he serve six months in jail.

On appeal defendant contends: his crime should not be a felony as the statute, section 502, subdivision (c)(2),

[1] Unspecified section references are to the Penal Code.

lacks a mens rea requirement; the statute is unconstitutionally vague; the trial court erred in admitting evidence of prior misconduct by defendant and in admitting printouts of computer access times; the trial court should have given a unanimity instruction; the trial court should have granted his motion to reduce the offense to a misdemeanor. For the reasons stated below, we will affirm the judgment.

TRIAL EVIDENCE

Our summary of the trial evidence will focus on the charge of which defendant was convicted, knowingly accessing and taking data from a computer system (§ 502. subd. (c)(2)). Defendant was charged with taking the source code of his former employer Network Translation Incorporated (NTI). Defendant did not testify at trial.

NTI was a company formed by John Mayes in January 1995 to market his product, Private Internet Exchange (PIX). PIX allowed a computer in a local computer network to access the Internet by virtue of assigning an Internet protocol address to the computer for the purpose of its Internet connection. PIX also functioned as a firewall, preventing people outside a company from accessing the company's computers over the Internet.

Mayes had the idea for PIX in March 1994. He hired Brantley Coile, the best programmer he knew, to write the original code. Coile wrote the source code from scratch. The first product was sold in December 1994. It received good reviews in the technical press. In early September 1995, Cisco indicated its interest in acquiring NTI.

NTI hired defendant as a sales engineer and technical support on October 4, 1995. At that time NTI was still a small company with five or six employees. Cisco acquired NTI by a stock exchange in late October 1995 for around $31 million. Mayes insisted that Cisco retain all NTI employees. After NTI was acquired by Cisco, NTI remained on the same business premises. The employees worked in close quarters.

As a technical support engineer, defendant had access to NTI's source code. In his job, he heard and answered customer complaints about PIX.

In December 1995 or January 1996, defendant began talking with his neighbor and friend Larry Coryell and Debbie Appler, a marketing person, about developing a product that would compete with and improve on PIX. Appler told defendant that he could not work for Cisco while developing a competing product. Defendant said he wanted to remain there until he earned some stock bonuses.

When defendant was hired by NTI, Andrew Foss was already working there. In March 1996 they together created a program to check stock quotes. In writing the program defendant had questions about strings library functions. In trying to answer the questions, defendant and Foss looked at an example in the Sun operating system source code version 4.1.3.

Foss was familiar with the Sun operating system because a prior employer of his had licensed it. It was highly controlled and his access to it was logged. The C. files had headers on them identifying them as copy-protected property of Sun Microsystems. It is a large code, probably involving millions of lines of programming.

Foss was surprised to see the Sun operating system on defendant's computer. He cautioned defendant that he should not use the code while doing Cisco business and should probably not even have it on Cisco's computer network. Defendant explained that he moved the code from his home directory when he stopped working for Sun. Foss had no reason to believe either that defendant had the code inadvertently or intentionally.

It is common for UNIX engineers to take their personal home directory computer files with them on leaving a job.

The Sun operating system was derived from Berkeley Software Distribution (BSD), but the two operating systems evolved to have different features. There is a free version of BSD available on the Internet for the taking. Foss was unaware to what extent there is an overlap between free BSD and Sun's operating system. He was unaware that any part of the Sun operating system 4.1.3 was released to the public.

Defendant acknowledged to Foss that what he had was the Sun operating system. He did not say to Foss it was free source code.

Beginning in April 1996, Coryell began writing code for defendant. Defendant gave Coryell hand-written block diagrams about how the product should work. After Coryell gave defendant code he had written, defendant sometimes asked for more features.

In about mid-July 1996, defendant told John Mayes that he was leaving NTI and Cisco. He said he was going to stay with a friend in Hawaii for three to six months and do nothing.

On August 12, 1996, defendant and Coryell networked three computers in Coryell's home. Coryell provided a Sun computer and defendant provided two PCs. They wanted to test the code that Coryell had written.

August 16, 1996, was defendant's last day at Cisco.

For health reasons Coryell stopped writing code for defendant in December 1996. Coryell knew defendant was working with other programmers.

The next time Mayes saw defendant was in May 1997 at a Las Vegas trade show called Interop. Mayes was part of Cisco's mergers and acquisitions team. In the start-up city area, he saw signs that looked like NTI signs at the Meridian booth. He walked to the booth wearing his Cisco badge. The people in the booth turned off all the computer screens. He turned and saw defendant. Mayes said the product, Aegis, looked a lot like PIX. Defendant said they were going after a different market.

Mayes reported this to Cisco and they obtained the Aegis product for evaluation. Johnson Wu, an original NTI employee, tested Aegis and wrote a message dated May 20, 1997, noting similarities between Aegis and PIX.

On August 8, 1997, San Jose police officers executed a search warrant for defendant's apartment. The search was coordinated by district attorney's investigator John Smith. Computer expert Gordon Galligher went along for technical assistance. His first job was to locate any Internet connection and disable it so no one could change defendant's computer from the outside while the search was in progress. Galligher observed that defendant had a local area network set up. It included two Sun workstations called Vette and Camaro. No monitor was attached to

Vette. The network also included a PC Windows system and the build computer. Galligher unplugged the wireless Internet connection.

Smith made a backup tape to copy the contents of the Windows computer. Smith did not want to seize the computers and shut down defendant's business. Officers had to get the proper tape in order to back up the build computer.

Investigator Smith wanted to look at the Sun machines. Defendant said they were just his target machines, which meant they represented the outside world in testing a firewall feature. Defendant said they had nothing on them. Smith entered a computer command that provided a listing of the directories on the Camaro computer. Galligher noticed two directors, both labeled "D.W.H. S.R.C. N.T.I." One was "2 dot 7 dot 6," the other was "2 dot 6 dot one o two."

Up to this point, defendant had been joking with the officers. He mentioned how he liked his 20-second commute from his bedroom to his office. Defendant stopped joking when they saw these files and just glared at the officers. Smith looked inside these directories and saw a number of source code files labeled dot C and dot H. Looking at copyright notices for Network Translation, Galligher offered the opinion that they were source code files. At that point Smith decided to seize the two Sun workstations.

The Sun workstations were evidence at trial. These files on the Camaro machine proved to be versions of NTI source code in existence about the time defendant stopped working for Cisco and NTI.

During the search, Smith asked defendant why those files were on his computer. Defendant said he always makes a backup of his home directory when he leaves a company to keep his standard start-up files. If he had copied Cisco source code, it was an accident. He denied using it to create his own product.

With the Camaro computer at the district attorney's office, investigator Smith used a UNIX file listing command that displayed and printed out the access times of all the files on the computer. There were several access dates to the PIX source code after August 16, 1996, when defendant stopped working for Cisco. UNIX only retains the last access time. Some source code files were accessed on December 5, 1996, other [sic] on May 15, 1997. So many files were accessed on December 5, 1996, that, in Galligher's opinion, it could have been the result of a global backup. The accesses on May 15, 1997, were more selective. The Ethernet driver file was accessed on May 15, 1997.

Galligher testified that when the source code files were accessed on the Camaro computer, it appeared the computer's clock was functioning properly.

Galligher acknowledges that the access times do not say who accessed the files and that various UNIX commands can access a file without a person actually looking at the contents of the file or knowing that he or she was accessing the file. Also, a systems administrator could change the time on a computer clock.

An evaluation of Aegis showed that Coryell wrote 21 of its files. What defendant wrote was low level driver code. In Galligher's opinion, Coryell was the principal developer of Aegis. Aegis and PIX had a common ancestry. He could not say Aegis was derived from PIX.

1. MENS REA REQUIREMENT

Section 502, subdivision (c)(2) defines as a public offense: "Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." A violation of section 502, subdivision (c)(2) is punishable alternately as a felony or a misdemeanor. (§ 502, subd. (d)(1).)[3]

On appeal defendant contends that "[b]ecause section 502(c)(2) contains no mens rea, it should not properly be punished as a felony." Defendant made the same argument in an unsuccessful motion for a new trial.

People v. Coria (1999) 21 Cal.4th 868 explained: "Generally, '"[t]he existence of a mens rea is the rule of, rather than the exception to, the principles of Anglo-American criminal jurisprudence." . . . ' (*People v. Simons* (1995) 9 Cal.4th 493, 519, citations omitted.) In other words, there must be a union of act and wrongful intent, or criminal negligence. (Pen. Code, § 20; *People v. Vogel* (1956) 46 Cal.2d 798, 801.) 'So basic is this requirement that it is an invariable element of every crime unless excluded expressly or by necessary implication.' (*People v.*

---

[3] Section 502, subdivision (d)(1) states: "1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment."

Vogel, supra, at p. 801, fn. omitted.) In addition, Penal Code section 26 provides that a person is incapable of committing a crime where an act is performed in ignorance or mistake of fact negating criminal intent; a crime cannot be committed by mere misfortune or accident. (*People v. Lopez* (1986) 188 Cal.App.3d 592, 597.)" (*Id.* at p. 876.)

In re Jorge M. (2000) 23 Cal.4th 866 stated, "the requirement that, for a criminal conviction, the prosecution prove some form of guilty intent, knowledge, or criminal negligence is of such long standing and so fundamental to our criminal law that penal statutes will often be construed to contain such an element despite their failure expressly to state it." (*Id.* at p. 872.)

Section 502, subdivision (c)(2) uses the word "knowingly," which identifies the mens rea involved in violating this subdivision. *People v. McDaniel* (1994) 22 Cal.App.4th 278 explained: "'"A requirement of knowledge is not a requirement that the act be done with any specific intent. . . . The word 'knowing' as used in a criminal statute imports only an awareness of the facts which bring the proscribed act within the terms of the statute. (Pen. Code, § 7, subd. 5.)"' (*People v. Lopez, supra*, 188 Cal.App.3d 592, 598; *People v. Calban, supra*, 65 Cal.App.3d 578, 584.) CALJIC No. 1.21 defines 'knowingly' as 'with knowledge of the existence of the facts in question. . . . ' This definition is consistent with that found in Webster's Third New International Dictionary Unabridged (1981), which defines 'knowing' as 'having or reflecting knowledge, information, or insight . . . ,' and 'knowingly' as 'in a knowing manner

. . . with awareness, deliberateness, or intention. . . . ' (At p. 1252.)" *Id.* at p. 285.)[3]

Defendant contends that the word "knowingly" only modifies "accesses" and not the rest of the crime. "Thus, the strict liability part of the statute occurs after the computer is 'knowingly' accessed. Any copying of data, even accident or inadvertent copying, becomes illegal at that point."

We disagree with defendant's reading of the statute. As stated above, "a crime cannot be committed by mere misfortune or accident." (*People v. Coria, supra*, 21 Cal.4th at p. 876.) Evidence of accidental copying would negate the mental element of section 502, subdivision (c)(2). We reject defendant's characterization of the statute as creating strict criminal liability.

2. CONSTITUTIONALITY OF STATUTE

On appeal defendant contends section 502 is unconstitutionally vague. He made the same argument in an unsuccessful motion for a new trail.

Tobe v. City of Santa Ana (1995) 9 Cal.4th 1069 explained: "A penal statute must define the offense with sufficient precision that 'ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement.'

---

[3] The jury here was erroneously instructed that a violation of section 502, subdivision (b)(2) involves the "specific intent to take, copy or make use of data without permission." Defendant does not complain of this error, which could only have benefited him.

[Citations.] 'The constitutional interest implicated in questions of statutory vagueness is that no person be deprived of "life, liberty, or property without due process of law," as assured by both the federal Constitution (U.S. Const., Amends V, XIV) and the California Constitution (Cal. Const., art. I, § 7).' [Citation.]

"To satisfy the constitutional command, a statute must meet two basic requirements: (1) The statute must be sufficiently definite to provide adequate notice of the conduct proscribed; and (2) the statute must provide sufficiently definite guidelines for the police in order to prevent arbitrary and discriminatory enforcement." (*Id.* at pp. 1106-1107.)

We review the statute with this in mind. Since section 502 is a long statute, we will summarize the pertinent parts, keeping in mind that defendant was charged with violating subdivision (c)(2) between November 1, 1995, and August 16, 1996.[4] In overview, the statute describes a number of computer crimes in somewhat overlapping language and also creates several exemptions from prosecution.

Subdivision (a) states: "(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer

[4] Subdivision references in this part are to section 502.

technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

"The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data."

What the statute prohibited was contained in eight parts of subdivision (c). The jury was only instructed about the crime with which defendant was charged, a violation of subdivision (c)(2). That subdivision prohibited at the time of the charged offense, "except as provided in subdivision (i) . . . [¶] (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." (Stats. 1989, ch. 1357, § 1, p. 5725.) The jury was instructed with the relevant statutory definitions orally and in writing.[5]

---

[5] In pertinent part, subdivision (b) states: "(1) 'Access' means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

"(2) 'Computer network' means any system that provides communications between one or more computer systems and input/output

(Continued on following page)

What defendant claims is vague is not the above-quoted definition of the crime, but the statute's description of an exception or exemption from prosecution. Former subdivision (i) created the following exceptions to the computer crimes defined in subdivision (c): "(1) Subdivision (c) does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment.

"(2) Paragraph (3) of subdivision (c) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer program, or data when acting outside the scope of his or her lawful

---

devices including, but not limited to, display terminals and printers connected by telecommunication facilities. [¶] . . . [¶]

"(4) 'Computer services' includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

"(5) 'Computer system' means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

"(6) 'Data' means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device. [¶] . . . [¶]

"(8) 'Injury' means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program."

employment, so long as the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or so long as the value of supplies or computer services, as defined in paragraph (4) of subdivision (b), which are used does not exceed an accumulated total of one hundred dollars ($100)." (Stats. 1989, ch. 1357, § 1, p. 5727; current subd. (h) is similar, but not identical.)

Former subdivision (i)(2) thus created a specific exception to the crime defined in subdivision (c)(3), which is: "Knowingly and without permission uses or causes to be used computer services." Subdivision (c)(3) is a broad prohibition – against unauthorized use of a computer.

By its own terms, former subdivision (i)(2) created an exception or exemption limited to the crime defined in subdivision (c)(3) and not the crime defined in subdivision (c)(2) as the unauthorized taking, copying, or using of computer data with which defendant was charged. However, this exemption in (i)(2) was expanded to other crimes in former subdivision (j) as follows. "No activity exempted from prosecution under paragraph (2) of subdivision (i) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs." (Stats. 1989, ch. 1357, § 1, p. 5727; this language is now found in subd. (i).)

It is this expanded exemption, applicable to (c)(2), that defendant argues to be unconstitutionally vague. He contends that there "exists no basis for a reasonable person to discern when his or her access to a computer or system 'incidentally violates' the statute. In addition, it provides no rational basis on which the prosecutor can make his or her decision to prosecute under the statute.

The statute can easily be violated by an unwitting computer user – by pushing the wrong button which causes information to be displayed, copied, or downloaded."

In former subdivision (i)(2), the Legislature deemed some violations of subdivision (c)(3) to be so trivial or de minimis as not to warrant criminal treatment, namely computer use, though outside the scope of employment, that either does not injure the employer or does not use $100 worth of supplies or services. Possible examples of this would be an employee who "surfs" the Internet when he or she has been told not to, or, as the prosecutor suggested, an employee who plays a computer game. In former subdivision (j), the Legislature extended this exemption from prosecution to the kind of trivial unauthorized computer use that is essentially a violation of (3), though it "incidentally violates" the more specific subdivisions (2), (4), or (7).[6] More specifically, as applied to subdivision (c)(2), former subdivision (j) was designed to exempt from prosecution a person who is primarily engaged in de minimis unauthorized use of his or her employer's computer services if this use "incidentally" involved taking, copying, or using data from a computer.

The jury was instructed along these lines. "However, any employee who accesses or uses his or her employer's computer system, computer network, computer program or data when acting outside the scope of his or her lawful employment is not guilty of violating section 502 if the following elements are satisfied:

---

[6] We neither quote nor discuss subdivisions (c)(4) and (7).

"One, such access or use without permission incidentally involves the taking, copying or making use of any data; [¶] two, the employee's activities do not cause an injury to the employer or another; and, [¶] three, the value of supplies and computer services which are used does not exceed an accumulated value of one hundred dollars."

Defendant complains that there is no precedent for determining what amounts to an incidental violation of another statute. In fact, this is a familiar concern of courts in determining whether a criminal defendant should be subject to multiple punishments under section 654. "Whether a course of criminal conduct is divisible and therefore gives rise to more than one act within the meaning of section 654 depends on the intent and objective of the actor. If all of the offenses were incident to one objective, the defendant may be punished for any one of such offenses but not for more than one." (*Neal v. State of California* (1960) 55 Cal.2d 11, 19.) The trial court must determine whether one offense "was merely incidental to the primary objective" of another offense. (*Id.* at p. 20.)

We conclude that the phrase "incidentally violates" in former subdivision (j), now subdivision (i), does not render the statute unconstitutionally vague. Section 502 is a complex statute. It defines several computer crimes and creates several exemptions from prosecution. The jury instruction in this case described the application of the exemption to the crime described in subdivision (c)(2). We conclude that the exemption in issue is sufficiently clear to avoid constitutional problems.

3. DEFENDANT'S PRIOR MISCONDUCT

On appeal defendant contends that the trial court erred in admitting evidence of his prior misconduct in possessing apparent source code from Sun Microsystems.

At a pre-trial hearing, the prosecution offered to prove that defendant was in possession of "the source code to version 4.1.3 of the Sun operating system." The prosecution made an offer of proof based on the anticipated testimony of Andrew Foss, a coworker of defendant who did not testify at the hearing. The prosecutor acknowledged that it was common for programmers to copy their personal data from their work computer when they leave a job. However, when Foss saw Sun's source code on defendant's Cisco computer, defendant explained that he had inadvertently copied it along with his personal data. Defendant gave the same explanation later when asked why he had NTI source code on his home computer. The prosecution contended that this testimony would prove that defendant did not inadvertently take the PIX source code.

Defendant objected that the witness could not positively state that defendant had Sun source code. Also, defendant allegedly took the Sun code years earlier. The prosecutor should not be able to offer the evidence until defendant offered the defense of inadvertence.

The trial court asked, "Isn't that all just a matter of proof? The proponent has the burden of proof of these things. . . . [¶] Obviously, if I grant the request, that's his burden. He has to prove exactly what you said. He has to prove that, in fact, it was source code which was not readily available, was protected. . . . If he doesn't prove that, then you are right; there is no value whatsoever. It's

not a prior act. . . . [¶] If it isn't said, then it has no relevancy. . . . [¶] . . . [¶] [U]nless you can prove it up, it has no value." The prosecutor asserted that he could call witnesses who would prove it up. The court ruled, "under 352 that it is admissible in the People's case in chief and it is relevant as it bears upon the issue as to intent, because it does negate the statement of inadvertence. The time frame is such where it is not too remote."

The Attorney General contends that defendant waived his pretrial objection to Foss's testimony by failing to renew it at trial. *People v. Crittenden* (1994) 9 Cal.4th 83, explained: "in *People v. Morris, supra*, 53 Cal.3d 152, 189-190, we concluded that if a motion to exclude evidence is made raising a specific objection, directed to a particular, identifiable body of evidence, at the beginning of or during trial at a time when the trial judge can determine the evidentiary question in its appropriate context, the issue is preserved for appeal without the need for a further objection at the time the evidence is sought to be introduced." (*Id.* at p. 127.) Here the trial judge heard an extensive offer of proof before ruling at the pre-trial hearing "under 352 that it is admissible in the People's case in chief and it is relevant." Under these circumstances, we conclude that defendant was not required to renew his objection at trial.

People v. Gibson (1976) 56 Cal.App.3d 119, 127, explained, "It is an established principle of evidence law that evidence of other criminal acts or misconduct of a defendant may not be admitted at trial when the sole relevance is to show defendant's criminal propensities or bad character as a means of creating an inference that defendant committed the charged offense. (Evid. Code, § 1101, subd. (a); *People v. Sam* (1969) 71 Cal.2d 194.)" (*Id.* at p. 127.) Evidence Code section 1101, subdivision (b),

authorizes admission of evidence of a defendant's other misconduct "when relevant to prove some fact (such as motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake or accident, . . .) other than his or her disposition to commit such an act." Upon appropriate objection, the trial court should consider whether evidence of the other misconduct is more prejudicial than probative. (Evid. Code, § 352.)[7] As the jury was instructed, it is the prosecutor's burden at trial to prove a defendant's prior misconduct by a preponderance of the evidence. (CALJIC No. 2.50.1; *People v. Carpenter* (1997) 15 Cal.4th 312, 381-382.) On appeal the question is whether the trial court abused its discretion in admitting evidence of other misconduct. (*People v. Kipp* (1998) 18 Cal.4th 349, 369, 371.)

Evidence of uncharged offenses may be admitted, but, as explained by *People v. Ewoldt* (1994) 7 Cal.4th 380 (*Ewoldt*): "Evidence of uncharged offenses 'is so prejudicial that its admission requires extremely careful analysis. [Citations.]' (*People v. Smallwood* (1986) 42 Cal.3d 415, 428; see also *People v. Thompson*, (1988) 45 Cal.3d 86, 109.) 'Since "substantial prejudicial effect [is] inherent in [such] evidence," uncharged offenses are admissible only if they have *substantial* probative value.' (*People v. Thompson* (1980) 27 Cal.3d 303, 318, italics in original, fn. omitted.)" (*Id.* at p. 404.)

---

[7] Section 352 states: "The court in its discretion may exclude evidence if its probative value is substantially outweighed by the probability that its admission will (a) necessitate undue consumption of time or (b) create substantial danger of undue prejudice, of confusing the issues, or of misleading the jury."

Ewoldt, supra, 7 Cal.4th 380, 399-401, overruled *People v. Tassell* (1984) 36 Cal.3d 77 and revitalized the doctrine of using prior misconduct to prove a common design or plan. *Ewoldt* differentiated among the types of evidence needed to prove intent, a common design or plan, and identity. "The least degree of similarity (between the uncharged act and the charged offense) is required in order to prove intent. [Citation.] [T]he recurrence of a similar result . . . tends (increasingly with each instance) to negative accident or inadvertence or self-defense or good faith or other innocent mental state, and tends to establish (provisionally, at least, though not certainly) the presence of the normal, i.e., criminal, intent accompanying such an act. . . . ' [Citation.] In order to be admissible to prove intent, the uncharged misconduct must be sufficiently similar to support the inference that the defendant '"probably harbor[ed] the same intent in each instance." [Citation.'" (*Id.* at p. 402.)

Defendant contends that "The prosecution produced no concrete evidence that the code seen by Mr. Foss was proprietary at the time he observed it in 1996." In fact, Andrew Foss testified as follows. When he and defendant were creating a stock quote program at Cisco, on defendant's work computer Foss saw "the source code for Sun Microsystems, Sun o. s. 413, I think it was." "The C. files all have headers on them, you know, 'property of Sun Microsystems' with their copyright and their confidentiality statement and 'do not copy' and all of that. It's pretty standard stuff in the code." He could not say how much overlap there was between free BSD and Sun's operating system, but "I can tell you what the header files say in Sun o. s., which is they certainly think they own it." Regarding Sun 413, "Sun very much considered everything [a former

employer] used in that to be their proprietary information. And we had a license and an escrow account and all of the overhead that entails to use it." Foss's testimony is further summarized above (*ante,* at p. 3).

Even if Foss were not certain that defendant had Sun source code, it was relevant that defendant was cautioned in March 1996 about possessing source code. As the prosecutor argued to the jury, Foss's warning occurred "only four months before he leaves. So even if he had accidentally taken the sun operating source code, the danger of accidents and inadvertence of something he shouldn't have had been freshly called to his mind. So he didn't take that inadvertently," referring to NTI source code.

Defendant also contends that the probative value of Foss's testimony was diminished because he remained a Cisco employee and owned about $4 million worth of Cisco stock. *Ewoldt, supra,* 7 Cal.4th 380 stated: "The probative value of evidence of uncharged misconduct also is affected by the extent to which its source is independent of the evidence of the charged offense. For example, if a witness to the uncharged offense provided a detailed report of that incident without being aware of the circumstances of the charged offense, the risk that the witness's account may have been influenced by knowledge of the charged offense would be eliminated and the probative value of the evidence would be enhanced." (*Id.* at p. 404.) This factor is not dispositive, however. In *Ewoldt,* the Supreme Court found no abuse of discretion in the trial court's admission of evidence of uncharged child molestation even though the victim's sister's accusations followed the victim's accusations. (*Id.* at p. 405.)

Foss's financial interests were not before the court at the time of its pretrial ruling. Defendant was free to argue their significance to the jury and he did so. He argued that every witness was a current or former Cisco employee with substantial stock holdings. This new evidence does not demonstrate that the trial court abused its discretion in admitting Foss's testimony about defendant's prior misconduct. We conclude that the trial court did not err in this ruling.

4. EVIDENCE OF COMPUTER RECORDS

On appeal defendant contends that the trial court erred in admitting computer printouts of when computer files were last accessed.

At a pretrial hearing defendant objected "that the date and time on that is hearsay. It is a statement generated by the computer being admitted . . . for the truth of the matter asserted. It's the computer saying the last time I was accessed was this date. And that is hearsay." Defendant asserted there was no applicable hearsay exception.

The prosecutor responded that documents are admissible if properly authenticated. It is a document, not a business record. The prosecutor's computer expert checked the computer clock and it was accurate. To the extent the printout is hearsay, it amounts to an admission by defendant.

The trial court stated: "This is a very hypertechnical objection. Because if the date and time is offered for the truth of the matter asserted, it is hearsay. But the problem in this analysis is simply this. There is no declarant. The declarant is the computer. It's not a person. So when

you are talking about hearsay, you are talking about an out-of-court statement by the declarant. And there is no declarant here. The computer made the date-and-time record.

"Now, if the computer is found to be functional, if the computer has been examined and it is found that the clock has not been tampered with, then it's just a question as to whether or not this is reliable evidence that the court can admit. But it's not, in my view, a statement made by anybody. It's a date and time left by a machine."

"And if, in fact, it can be established by a foundation that the computer was functioning appropriately, had not been tampered with, and the clock was accurate, in the court's view, especially in view of what's happening in our modern society with technology and computers and so on, in the court's view that would be credible, reliable evidence that the computer was working, the clock was accurate, it hadn't been tampered with, and this was the date and time the computer left with respect to when a file was accessed. If we couldn't do that, it would seem to the court that it would be impossible under most circumstances to have anything introduced by way of a computer record simply on the basis that it's hearsay. And the declarant is the computer. And the computer can't be cross-examined.

"So, my inclination would be that this is admissible. And I can't really tell you why, other than if the computer was working, it can be verified it was working, it can be verified it was functional and accurate; that that date and time left in a person's computer is admissible evidence. Now, I can't give you chapter and verse as to what it's

called, why it's admissible, but simply in the court's view it would be because it's reliable and it's credible."

Defendant asked to have a continuing objection at trial and the court "so noted."

We have summarized above (*ante*, at p. 5) the testimony of computer expert Gordon Galligher about the computer file access times found on defendant's computer. After finding what appeared to be NTI source code on defendant's Camaro computer, he had investigator Smith use a UNIX command to display when the files had last been accessed. Several files were accessed after August 16, 1996, when defendant stopped working for NTI. A large number of files were accessed last on December 5, 1996, while a smaller number were accessed on May 15, 1997. As far as Galligher could tell, the computer clock was operating properly when the files were accessed.

Galligher acknowledged that the access times do not say who accessed the files and that various UNIX commands can access a file without a person actually looking at the contents of the file or knowing that he or she was accessing the file. Also, a systems administrator could change the time on a computer clock.

When the prosecutor offered the computer printouts into evidence, defendant counsel reminded the court there was a standing objection.

Defendant renews his hearsay objection on appeal. He contends that the computer printouts of the access dates do not qualify as business records under Evidence Code section 1271, which states: "Evidence of a writing made as

a record of an act, condition, or event is not made inadmissible by the hearsay rule when offered to prove the act, condition, or event if:

"(a) The writing was made in the regular course of a business;

"(b) The writing was made at or near the time of the act, condition, or event;

"(c) The custodian or other qualified witness testifies to its identity and the mode of its preparation; and

"(d) The sources of information and method and time of preparation were such as to indicate its trustworthiness."

California cases have held computer printouts admissible when they fit within a hearsay exception as business records (*People v. Lugashi* (1988) 205 Cal.App.3d 632, 641-642) or official records (*People v. Martinez* (2000) 22 Cal.4th 106, 126-134). In *Aguimatang v. California State Lottery* (1991) 234 Cal.App.3d 769, the court stated that if computer printouts are "offered for the truth, . . . they must qualify under some hearsay exception, such as business records under Evidence Code section[] 1271. . . . (Jefferson, Cal. Evidence Benchbook (2d ed. 1982) Vol. 1, § 4.3, pp. 236-237.)" (*Id.* at p. 797, fn. omitted.)

As defendant points out, these cases have not discriminated among the different types of information that computers can print out. A computer can be used to store documents and information entered by human operators. A computer can also be programmed to generate information on its own, such as a record of its internal operations. Some jurisdictions have recognized that the latter type of

computer-generated information is not hearsay because it is not a statement by a person.

"'Hearsay evidence' is evidence of a statement that was made other than by a witness while testifying at the hearing and that is offered to prove the truth of the matter stated." (Evid. Code, § 1200, subd. (a).) "'Statement' means (a) oral or written verbal expression or (b) nonverbal conduct of a person intended by him as a substitute for oral or written verbal expression." (Evid. Code, § 225.) "'Person' includes a natural person, firm, association, organization, partnership, business trust, corporation, limited liability company, or public entity." (Evid. Code, § 175.) The Evidence Code does not contemplate that a machine can make a statement.

The leading case of *State v. Armstead* (La.Ct.App. 1983) 432 So.2d 837 explained: "The printout of the results of the computer's internal operations is not hearsay evidence. It does not represent the output of statements placed into the computer by out of court declarants. Nor can we say that this printout itself is a 'statement' constituting hearsay evidence. The underlying rationale of the hearsay rule is that such statements are made without an oath and their truth cannot be tested by cross-examination. [Citations.] Of concern is the possibility that a witness may consciously or unconsciously misrepresent what the declarant told him or that the declarant may consciously or unconsciously misrepresent a fact or occurrence. . . . [Citations.] With a machine, however, there is no possibility of a conscious misrepresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly." (*Id.* at p. 840; cf. *Ly v. State* (Tex.App. 1995) 908 S.W.2d 598, 600.) "The role that the hearsay rule plays in limiting the fact

finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy." (*State v. Meeks* (Tenn. 1993) 867 S.W.2d 361, 376; cf. *State v. Dunn* (Miss. 1999) 7 S.W.2d 427, 431-432.)

We agree with this authority. As the trial judge in this case perceived, the true test for admissibility of a printout reflecting a computer's internal operations is not whether the printout was made in the regular course of business, but whether the computer was operating properly at the time of the printout. The trial court did not err in rejecting defendant's hearsay objection and admitting the printouts into evidence.

Evidence Code section 1552 (formerly section 1500.5) states: "(a) A printed representation of computer information or a computer program is presumed to be an accurate representation of the computer information or computer program that it purports to represent. This presumption is a presumption affecting the burden of producing evidence. If a party to an action introduces evidence that a printed representation of computer information or computer program is inaccurate or unreliable, the party introducing the printed representation into evidence has the burden of proving, by a preponderance of evidence, that the printed representation is an accurate representation of the existence and content of the computer information or computer program that it purports to represent."

This presumption operates to establish only that a computer's print function has worked properly. The presumption does not operate to establish the accuracy or reliability of the printed information. On that threshold issue, upon objection the proponent of the evidence must offer foundational evidence that the computer was operating properly.

On appeal defendant also contends that the prosecutor failed to establish the reliability of the information pertaining to the access times of the computer files. "[T]he testimony of Mr. Galligher made it clear that there were many ways in which the access date information could have been generated. . . . [I]n light of Mr. Galligher's testimony, the source, method and time of preparation were not such as to indicate trustworthiness."

In the trial court defendant objected that the printouts were hearsay, but not that they were unreliable. We note that the trustworthiness of a writing is one aspect that makes it admissible as a business record. But defendant did not specifically object in the trial court that the time and date were inaccurate. Accordingly, this objection is unavailable on appeal. (Evid. Code, § 353, subd. (a).)

Because defendant did not specifically object to reliability, the trial judge did not have much information on this topic at the time he ruled the printouts admissible. Based on the prosecutor's offer of proof that the computer clock was functioning properly, the trial court did not err in its ruling.

Defendant also contends that the trial evidence of the printouts was so unreliable as to deny his constitutional right to a fair trail. Defendant cites *People v. Hernandez* (1997) 55 Cal.App.4th 225 in support. That case concluded

that a defendant was prejudiced when a police department crime analyst testified about the results of her computer search of police records of sex crimes similar to those with which the defendant was charged. The appellate court concluded: "Under the circumstances of this case, where the outcome of the trial turned on the credibility of the two victims, whose descriptions of their attacker varied before and at trial and contained many inconsistencies and contradictions, we cannot say the trial court's error in admitting the analyst's testimony was harmless. (*People v. Watson* [(1956)] 46 Cal.2d [818] at p. 836.) The devastating effect on Hernandez's right to a fair trial by the admission of such 'pseudo-scientific' testimony, which basically elevated multiple layers of hearsay spit out by a computer system named Sherlock to truth, to bolster such credibility cannot be overstated." (*Id.* at pp. 243-244.) *Hernandez* found prejudice under a *Watson* standard, not the denial of a fair trial. It is factually dissimilar to our case. It involved computer-stored information, not computer-generated information.

Defendant suggests that this evidence of computer access times was so bad as to have compromised any chance of a fair trial. In our view, the jury was well aware of the limited value of this evidence. There was substantial testimony about how computer files could be accessed and whether access times could be manipulated.

The prosecutor's opening argument to the jury asserted in part: "[UNIX] records a great deal of information, but it doesn't record every access. We can only go by the last access. Something happened with these files on December 5th. And it didn't happen globally. It wasn't like he backed up every file in that system, because the files bear different access dates. He did something special with

both the source code files on December 5th. In May 1997, he did something special with 2.6.102 file. He tagged every one that is actually a source code file. Headers and source code file, but not the others that are there in 2.6.102."

"And with 2.7.6, we have maybe the most striking evidence in the case. The area he accessed one file on that date, May 17th [*sic*] 1997, concerning the Ethernet card, the famous 3C509 or 590, and all of the files that were changed in the Aegis source code are related to Ethernet problems. That is proof positive that the source code file was accessed after he left and used."

In response defendant argued: "The access date argument is based on a clock. And there's been testimony regarding the clock and whether it's reliable. The testimony is that it can be changed by the user. It can be changed by modifying the clock. That anyone who has root access to a computer can change the access times." Anybody on that computer had root access. Also files can be accessed "by commands that don't imply actual human access." "There has been no evidence in this case whatsoever, zero, as to who did whatever was done that created those access times."

In closing argument, the prosecutor pointed out that the computer containing the source code was found in defendant's apartment.

The jury was informed that the computer printouts listing the access times of computer files only purported to show when files were last accessed, not how, why, or by whom. A computer expert explained to the jury how the time could be changed. Contrary to defendant's characterization, the expert's testimony did not establish "that the dates on the printouts were unreliable." These limits on

the probative value of these printouts affected their weight, not their admissibility. (*People v. Martinez, supra,* 22 Cal.4th at p. 132.) We conclude that admission of this evidence was not error and it neither prejudiced defendant nor deprived him of a fair trial.

5. UNANIMITY

On appeal defendant contends that the trial court erred by failing to give a unanimity instruction sua sponte such as CALJIC No. 4.71.5. The jury should have been instructed that since defendant was charged with committing a crime between November 1, 1995, and August 16, 1996, the jury had to unanimously agree that the prosecutor had proved that defendant committed a specific act or acts constituting the crime within that time period.

People v. Russo (2001) 25 Cal.4th 1124 is instructive. "In a criminal case, a jury verdict must be unanimous. (*People v. Collins* (1976) 17 Cal.3d 687, 693; see Cal. Const., art. I, § 16 [expressly stating that 'in a civil cause three-fourths of the jury may render a verdict' and thereby implying that in a criminal cause, only a unanimous jury may render a verdict].) . . . Additionally, the jury must agree unanimously the defendant is guilty of a specific crime. (*People v. Diedrich* (1982) 31 Cal.3d 263, 281.) Therefore, cases have long held that when the evidence suggests more than one discrete crime, either the prosecution must elect among the crimes or the court must require the jury to agree on the same criminal act. (*People v. Castro* (1901) 133 Cal. 11, 13; *People v. Williams* (1901) 133 Cal. 165, 168; CALJIC No. 17.01; but see *People v. Jones* (1990) 51 Cal.3d 294.)

"This requirement of unanimity as to the criminal act 'is intended to eliminate the danger that the defendant will be convicted even though there is no single offense which all the jurors agree the defendant committed.' (*People v. Sutherland* 1993) 17 Cal.App.4th 602, 612.) For example, in *People v. Diedrich, supra,* 31 Cal.3d 263, the defendant was convicted of a single count of bribery, but the evidence showed two discrete bribes. We found the absence of a unanimity instruction reversible error because without it, some of the jurors may have believed the defendant guilty of one of the acts of bribery while other jurors believed him guilty of the other, resulting in no unanimous verdict that he was guilty of any specific bribe. (*Id.* at pp. 280-283.) 'The [unanimity] instruction is designed in part to prevent the jury from amalgamating evidence of multiple offenses, no one of which has been proved beyond a reasonable doubt, in order to conclude beyond a reasonable doubt that a defendant must have done something sufficient to convict on one count.' (*People v. Deletto* (1983) 147 Cal.App.3d 458, 472.)

"On the other hand, where the evidence shows only a single discrete crime but leaves room for disagreement as to exactly how that crime was committed or what the defendant's precise role was, the jury need not unanimously agree on the basis or, as the cases often put it, the 'theory' whereby the defendant is guilty. (See generally *People v. Jenkins* (2000) 22 Cal.4th 900, 1024-1026.) The crime of burglary provides a good illustration of the difference between discrete crimes, which require a unanimity instruction, and theories of the case, which do not. Burglary requires an entry with a specified intent. (Pen. Code, § 459.) If the evidence showed two different entries with burglarious intent, for example, one of a house on

Elm Street on Tuesday and another of a house on Maple Street on Wednesday, the jury would have to unanimously find the defendant guilty of at least one of those acts. If, however, the evidence showed a single entry, but possible uncertainty as to the exact burglarious intent, that uncertainty would involve only the theory of the case and not require the unanimity instruction. (*People v. Failla* (1966) 64 Cal.2d 560, 567-569.) Other typical examples include the rule that, to convict a defendant of first degree murder, the jury must unanimously agree on guilt of a specific murder but need not agree on a theory of premeditation or felony murder (*People v. Pride* (1992) 3 Cal.4th 195, 249-250), and the rule that the jury need not agree on whether the defendant was guilty as the direct perpetrator or as an aider and abettor as long as it agreed on a specific crime (*People v. Santamaria* (1994) 8 Cal.4th 903, 918-919)." (*Id.* at pp. 1132-1133.)

Defendant contends that "the prosecutor pointed to two separate set[s] of facts in arguing that appellant was guilty of Count Two. The first was that the source code was found on appellant's personal computer. This, argued the prosecution was evidence that appellant intentionally *copied* the code and *took* it from Cisco. Next, the prosecution pointed to the UNIX dates as evidence that a year after leaving Cisco appellant *accessed* the source code and *used* the date to construct his own product. Each set of facts argued by the prosecution, if found true by the jury, could constitute a violation of section 502(c)(2). Yet these two acts occurred on different dates."

The Attorney General seemingly agrees, "some of the jurors in this case could have convicted appellant of violating section 502 on the theory that he copied the [PIX] source codes, while others convicted him on the theory

that he simply made use of the source codes. Still others could have convicted him on the theory that he took the source codes with him when he left Cisco." The Attorney General contends that "these potential differences in theories of liability do not warrant an instruction on unanimity because the jury was ultimately unanimous that appellant committed a single violation of section 502 involving the [PIX] source code." "[E]ven if jurors in this case relied on different facts underlying the various theories of liability, they ultimately agreed that appellant committed a violation" of the statute.

Our review of the record shows that in argument to the jury the prosecutor elected what act amounted to the violation of section 502. Moreover, as the jury was instructed, defendant was charged with violating this statute between November 1, 1995 and August 16, 1996, while he was working for NTI. Evidence that someone accessed the source code on his home computer in May 1997 falls outside the charged crime.

In opening argument, the prosecutor said, "Despite the technical background of this case, this is actually a fairly easy case. It involves theft. Two kinds of theft. One of trade secrets. Actually, it's the same theft charged two different ways: one of a trade secret; one of a simple copying." The second count is "what I call the easy count." The prosecutor read the definition of the crime and argued: "I have no problem with [']knowingly accesses.['] [Defendant] knew of the network, knew of the system. He knows when he's making the copy that he's making the copy. And that's what – actually, there is a definition of [']accesses,['] and you'll find that's exactly what it means.

"And there is no real problem [']without permission.[']
That source code was never intended to leave Cisco."
"[']Takes, copies, or makes use of[']it. He took it. He made a copy of it. He made use of it." The prosecutor argued that if defendant had taken it inadvertently, he would not have accessed it later.

"So let me summarize that as the easy count, other than that one. All we have to do is show that he copied and he copied with the specific intent knowing he was copying, knowing that he was taking. We don't have to show what he did with it afterwards. Just that he took it, knowing that he was taking it with the specific intent to take, copy or make use of data."

Later in opening argument, the prosecutor stated, "Count two, the illicit copy, all we have to do is show that he took that data knowing he was taking it."

In closing argument, the prosecutor stated, "Count two is almost like count one, with one element missing. He copied the access, knowingly accessed the Cisco computer and without permission took, copied that data, copied and moved it to his own computer, thereby completing a crime. And it wasn't inadvertent. It wasn't an accident. He did it on purpose, because he needed it. That's our case."

This was not a case where the prosecutor asked the jurors to select from among several discrete acts by defendant in order to convict him of violating section 502, subdivision (c)(2). Rather, the prosecutor repeatedly asserted in argument to the jury that the crime was completed when defendant copied his employer's source code files and took them home for installation on his home computer. The prosecutor did not rely on defendant's alleged later use of the source code as a separate violation

of subdivision (c)(2). While defendant's conduct may be characterized as copying or taking, in fact his conduct amounted to both. Under the evidence offered, no juror could have found that defendant took the source code without copying it. Because the prosecutor's opening argument elected what conduct by defendant amounted to the crime charged, we conclude that no unanimity instruction was required. (*People v. Diaz* (1987) 195 Cal.App.3d 1375, 1383.)

In light of this conclusion, we need not consider whether defendant was involved in a continuous course of conduct or whether defendant was prejudiced by the lack of a unanimity instruction.

6. FELONY OR MISDEMEANOR

As noted above, a violation of section 502, subdivision (c)(2) is punishable alternately as a felony or a misdemeanor. (§ 502, subd. (d)(1).) After trial, defendant made a motion to reduce his conviction to a misdemeanor under section 17, subdivision (b). Defendant's motion was based on the statute's alleged vagueness and lack of a mens rea requirement. We have rejected both arguments above.

On appeal defendant contends that the trial judge might have relied on impermissible considerations in denying his motion to reduce the offense. This contention depends on the following facts.

In connection with defendant's sentencing, he submitted a 43-page typed document entitled "My Side Of The Story." The prosecutor responded to this document, writing that it demonstrated no remorse. "The defendant, who presented no defense and submits his statement ex parte,

without exposing himself to cross-examination, has no inhibitions about casting aspersions on the credibility of everyone who did testify.1" In footnote 1, the prosecutor wrote, "Had the defendant submitted no statement, the People would have remained silent on this point. However, since he chose to do so, and to do so in a manner that circumvents any challenge by cross-examination, comment on his methods is fair. The contrast between the extensive, time consuming examination he imposed upon all prosecution witnesses and his own reluctance to be tested in the same manner, is striking."

At the hearing on defendant's motion, his attorney stated, "I was quite taken aback at Mr. Berry's response to our motion for a new trial in the degree to which he seems to take umbrage with Mr. Hawkins exercising his constitutional right to remain silent, his constitutional right to cross-examine witnesses, his constitutional right to allocute and submit a sentencing statement." The district attorney was attacking defendant "for exercising those constitutional rights."

The prosecutor essentially reiterated his response. Defense counsel asserted that defendant had acknowledged that he would change his conduct.

The court ruled as follows. "I'm not going to make a lot of comments, but I didn't glean that from his statement [sic] remorse for what he did. I gleaned more remorse for the fact that he found himself in a situation he didn't want to be in for conduct that he felt was not really culpable."

After denying the new trial motion, the court stated. "The motion to reduce pursuant to Penal Code section 17 is denied in the exercise of the court's discretion. I don't feel it's an appropriate case for a reduction for Penal Code

section 17." The judge agreed with the jury based on the evidence that "it wasn't accidental. It wasn't inadvertent." When the police executed the search warrant, defendant "knew that the source code from Cisco would be on his computer. And he reacted in a fashion which indicated to the court and to the jury, I'm sure, a consciousness of guilt; that he'd been caught. He did exactly what he was charged with doing. He left Cisco, and at the time he left he had accessed the computer at Cisco. And when he downloaded his information, he took with him the source code. And he knew exactly what he was doing. And I think the jury found that. So, there is no question but that he's culpable.

"His statement to me through the probation department as to what happened is something he could have told the jury. He had an absolute right to remain silent and not testify, and that's a choice and decision he made. He's not going to be penalized for that. But, on the other hand, I'm not going to sit here now as a judge and say, well, if he had said this to the jury, they would have done something differently. The jury decided the case based on what they had, and I believe the evidence is more than sufficient to support the finding." What defendant did is prohibited by the statute.

"So far that reason, again, the motion under 17 was denied and the motion for new trial was denied, because I think the statute is, in fact, clear as to what the prescribed conduct is as to probation versus prison."

Defendant suggests that the trial court "improperly consider[ed] [defendant's] silence at trial in denying" his motion. (Capitalization omitted.) We see no evidence that the trial court did not mean what it said about not penalizing defendant for remaining silent. Defendant also

contends that the trial court erred by ignoring defendant's allocution. In fact, the court expressly discussed whether defendant's written statement exhibited remorse.

Trial courts have broad authority in ruling on motions under section 17 to reduce a crime to a misdemeanor. (*People v. Superior Court (Alvarez)* (1997) 14 Cal.4th 968, 977.) We conclude that defendant has not demonstrated that the trial court abused its discretion in denying his motion.

DISPOSITION

The judgment is affirmed.

BAMATTRE-MANOUKIAN, ACTING P.J.

WE CONCUR:

MIHARA, J.

RUSHING, J.

COPY

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE
STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

THE PEOPLE, Plaintiff and Respondent, v. DAVID WESLEY HAWKINS, Defendant and Appellant.	H021902 (Santa Clara County Super. Ct. No. 210319) ORDER MODIFYING OPINION AND DENYING REHEARING **[NO CHANGE IN JUDGMENT]** (Filed Jul. 2, 2002)

THE COURT:

It is ordered that the opinion filed herein on June 5, 2002, be modified in the following particulars:

1. On page 9, line 4 of the fourth full paragraph, delete the reference to "subdivision (i)" and replace with subdivision (h).

2. On page 10, line 1, beginning "(Stats. 1989, ch. 1357, § 1, p. 5725.)" is deleted and the following is inserted in its place:

(Stats. 1989, ch. 1357, § 1.3, p. 5738.)

3. On page 10, line 3 of the first full paragraph, delete the reference to "subdivision (i)" and replace with subdivision (h).

4. On page 11, line 5 of the first paragraph, beginning "(Stats. 1989, ch. 1357, § 1, p. 5727" is deleted and the following is inserted in its place.

(Stats. 1989, ch. 1357, § 1.3, p. 5740

5. On page 11, line 1 of the first paragraph, delete the reference to "subdivision (i)(2)" and replace with subdivision (h)(2).

6. On page 11, the second full paragraph is deleted and the following is inserted in its place:

By its own terms, former subdivision (h)(2) created an exception or exemption limited to the crime defined in subdivision (c)(3) and not the crime defined in subdivision (c)(2) as the unauthorized taking, copying, or using of computer data with which defendant was charged. However, this exemption in (h)(2) was expanded to other crimes in subdivision (i) as follows. "No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs." (Stats. 1989, ch. 1357, § 1.3, p. 5740.)

7. On page 11, line 1 of the fourth full paragraph, delete the reference to "subdivision (i)(2)" and replace with subdivision (h)(2).

8. On page 12, line 6 of the first paragraph, delete the words "former subdivision (j)" and replace with subdivision (i).

9. On page 13, first full paragraph, delete the first sentence beginning with "We conclude" and insert the following so the sentence reads:

We conclude that the phrase "incidentally violates" in subdivision (i) does not render the statute unconstitutionally vague.

10. On page 17, at the end of the third full paragraph, after the sentence ending "no applicable hearsay exception" add the following sentence, including the footnote, so the sentence reads:

Defendant contended that computer dates and times were notoriously unreliable and that reliability had to be established.[8]

11. On page 21, delete the fourth full paragraph in its entirety.

12. On page 21, delete the first sentence of the fifth full paragraph beginning with "Because defendant" and insert the following sentence in its place so the sentence reads:

The trial judge did not have much information on the topic of reliability at the time he ruled the printouts admissible.

The petition for rehearing is denied.

---

[8] The reporter's transcript attributed these statements to the prosecutor, but from the context it appears they were made by defense counsel.

This modification does not effect a change in the judgment.

BAMATTRE-MANOUKIAN, ACTING P.J.

MIHARA, J.

RUSHING, J.

People v. Hawkins
H021902

Court of Appeal, Sixth Appellate District – No. H021902
S108293

IN THE SUPREME COURT OF CALIFORNIA

En Banc

THE PEOPLE, Plaintiff and Respondent,

v.

DAVID WESLEY HAWKINS, Defendant and Appellant.

(Filed Aug. 28, 2002)

Petition for review DENIED.

Kennard, J., is of the opinion the petition should be granted.

GEORGE
Chief Justice